UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,651	01/30/2006	Kazuo Omori	SONY JP 3.3-328	2255

530 7590 05/11/2009

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
SU, SARAH	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
05/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,651	OMORI ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☒ Claim(s) *2-4,7,11 and 12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 12 December 2008, has been entered into record. In this amendment, claims 1-14 have been amended, and claims 15-22 have been added.

2. Amendment B, received on 13 February 2009, has been entered into record. In this amendment, claims 1, 3-11, 13, 14 have been amended, and claims 23-30 have been added.

3. Claims 1-30 are presented for examination.

Response to Arguments

4. With regards to the objection to the drawings, the applicant has submitted replacement drawings, and the examiner hereby withdraws the objection.

5. Applicant's arguments and amendments with respect to the rejection under 35 USC 112, second paragraph of claims 1, 5, 7, 10, 13, and 14 have been fully considered and are persuasive. The rejection of 9 July 2008 has been withdrawn.

6. Applicant's arguments and amendments with respect to the rejection under 35 USC 101 of claims 9 and 14 have been fully considered and are persuasive. The rejection of 9 July 2008 has been withdrawn.

7. Applicant's arguments with respect to claims 1-14 have been considered but are moot in view of the new ground(s) of rejection.

Specification

8. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 9 and 14 disclose "A program on a computer readable medium." The specification is objected to because the "computer readable medium" is not defined in the specification.

Claim Objections

9. Claims 2-4, 7, 11, and 12 are objected to because of the following informalities:

a. In claims 2-4, line 1: "A data processing method" is unclear if it relates to "A data processing method" (claim 1, line 1);

b. In claim 7, line 1: "A data processing method" is unclear if it relates to "A data processing method" (claim 6, line 1);

c. In claims 11 and 12, line 1: "A data processing method" is unclear if it relates to "A data processing method" (claim 1, line 1);

Appropriate correction is required.

Drawings

10. The drawings were received on 12 December 2008. These drawings are acceptable.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oishi et al. (EP 1037131 A2 and Oishi hereinafter) and in view of Stirbu (US 2003/0200433 A1).

As to claims 1, 8, 9, 23, and 27, Oishi discloses a system and method for mutual identification between apparatuses, the system and method having:

> **a second step by which, when the second data processing device verifies the first data processing device by the authentication in the first step, the first processing device uses the encryption key data for encryption** (0120, lines 1-3) **and the second processing device decrypts encrypted data provided to the second data processing device by using the decryption key data** (0122, lines 1-3)**,**
>
> **a third step by which, when the second data processing device judges that decryption data obtained by the decryption in the second step is decrypted adequately, the second data processing device uses the decryption data as the data that is effective** (i.e. legitimate) (0107, lines 1-6)**.**

Oishi fails to specifically disclose:

a first step by which the first data processing device uses the first authentication key data, wherein the first authentication key data is from an integrated circuit ("IC") device and had been generated using predetermined key data, and the second processing device uses the second authentication key data, wherein the second authentication key data is generated using key data designated by key designation data, wherein the key designation data is from the IC device, and authentication is performed between the first data processing device and the second data processing device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Oishi, as taught by Stirbu.

Stirbu discloses a system and method for providing peer authentication for an internet key exchange, the system and method having:

a first step by which the first data processing device (i.e. initiator) **uses the first authentication key data, wherein the first authentication key data** (i.e. key) **is from an integrated circuit ("IC") device and had been generated using predetermined key data** (i.e. from manufacturer) (0033, lines 1-8)**, and the second processing device** (i.e. responder) **uses the second authentication key data** (i.e. derived information)**, wherein the second authentication key data is generated using key data designated by key designation data** (i.e. secret key)**, wherein the key designation data is from the IC device, and authentication is performed between the first data**

processing device and the second data processing device (0033, lines 9-14).

Given the teaching of Stirbu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Oishi with the teachings of Stirbu by using information from an integrated circuit to perform authentication between processing devices. Stirbu recites motivation by disclosing that transmitting key data "out-of-band" prevents eavesdropping, but authentication does not rely on keeping secret the identity associated with a private key (0004, 1-4, 14-17). Stirbu also discloses that authentication of an initiator and responder based on information based on an unrevealed secret key provides for phase 1 authentication on already implemented infrastructure (0012, lines 6-11). It is obvious that the teachings of Stirbu would have improved the teachings of Oishi by performing authentication using information provided by a third party in order to implement phase 1 authentication that relies on keeping secret an identity using already implemented infrastructure.

As to claim 2, Oishi discloses:

in the first step, the first data processing device and the second data processing device perform encryption and decryption of predetermined data based on a first encryption algorithm and a first decryption algorithm corresponding to the first encryption algorithm and perform the authentication (0027, lines 1-3; 0120, lines 1-3; 0122, lines 1-3),

in the second step, the second data processing device decrypts the encrypted data encrypted based on a second encryption algorithm based on a second decryption algorithm corresponding to the second encryption algorithm (0027, lines 1-3; 0149, lines 1-4).

As to claims 3, 25, and 29, Oishi discloses:

wherein the first data processing device is verified in the second step, when the second data processing device judges that the first authentication key data and the second authentication data are the same by the authentication in the first step (0107, lines 1-6).

As to claims 4, 26, and 30, Oishi discloses:

a fourth step by which the first data processing device (i.e. portable player) **provides the key designation data** (i.e. random number) **designating the predetermined key data used for generation of the first authentication key data to the second data processing device** (i.e. portable storage device) (0096, lines 3-6),

a fifth step by which the second data processing device generates the second authentication key data by a second predetermined generation method by using the predetermined key data designated by the key designation data received in the fourth step (0096, lines 7-11),

a sixth step by which the first data processing device uses the first authentication key data and uses the second authentication key data

generated by the second data processing device in the fifth step to perform the authentication (0099, lines 1-2)**,**

a seventh step by which when the second data processing device judges that the first authentication data and the second authentication data are the same, the first data processing device is verified (0107, lines 1-6)**.**

As to claim 5, Oishi discloses:

wherein the first data processing device uses the first authentication key data and the second data processing device uses the second authentication key data, and an authentication is performed between the first data processing device and the second data processing device (0120, lines 1-3; 0122, lines 1-3)**,**

the second data processing device decrypts encrypted data provided to the second data processing device by the first data processing device by using the encryption key data for encryption by using the decryption key data, when the second data processing device verifies the first data processing device by the authentication (0149, lines 1-4)**,**

the second data processing device uses the decryption data as the data that is effective, when the second data processing device judged decryption data obtained by the decryption is decrypted adequately (0107, lines 1-6)**.**

Oishi fails to specifically disclose:

a first data processing device holding first authentication key data and encryption key data, wherein the first authentication key data is from an integrated circuit ("IC") device and had been generated using predetermined key data,

a second data processing device holding second authentication key data corresponding to the first authentication key data, and decryption key data corresponding to the encryption key data, wherein the second authentication key data is generated using key data designated by key designation data, wherein the key designation data is from the IC device.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Oishi, as taught by Stirbu.

Stirbu discloses:

a first data processing device (i.e. initiator) **holding first authentication key data** (i.e. key) **and encryption key data** (i.e. MAC), **wherein the first authentication key data is from an integrated circuit ("IC") device and had been generated using predetermined key data** (0033, lines 1-8; 0034, lines 15-18; 0036, lines 1-6),

a second data processing device (i.e. responder) **holding second authentication key data** (i.e. derived information) **corresponding to the first authentication key data, and decryption key data corresponding to the encryption key data, wherein the second authentication key data is**

generated using key data designated by key designation data, wherein the key designation data is from the IC device (0033, lines 9-14; 0035, lines 2-4).

Given the teaching of Stirbu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Oishi with the teachings of Stirbu by using data from an integrated circuit to authenticate processing devices. Please refer to the motivation recited above with respect to claim 1 as to why it is obvious to apply the teachings of Stirbu to the teachings of Oishi.

As to claim 6, Oishi discloses:

a second step of encrypting predetermined data by using the encryption key data after the authentication in the first step (0120, lines 1-3),

a third step of outputting data obtained from the encryption in the second step to the authenticated side (0120, lines 1-3).

Oishi fails to specifically disclose:

a first step of performing authentication with an authenticated side by using the first authentication key data, wherein the first authentication key data is from an integrated circuit ("IC") device and had been generated using predetermined key data, and wherein the authentication side uses second authentication key data generated using key data designated by key designation data from the IC device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Oishi, as taught by Stirbu.

Stirbu discloses:

> **a first step of performing authentication with an authenticated side by using the first authentication key data** (i.e. key)**, wherein the first authentication key data is from an integrated circuit ("IC") device and had been generated using predetermined key data, and wherein the authentication side uses second authentication key data** (i.e. derived information) **generated using key data designated by key designation data from the IC device** (0033, lines 1-14)**.**

Given the teaching of Stirbu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Oishi with the teachings of Stirbu by using data from an integrated circuit to authenticate processing devices. Please refer to the motivation recited above with respect to claim 1 as to why it is obvious to apply the teachings of Stirbu to the teachings of Oishi.

As to claim 7, Oishi discloses:

> **a fourth step of providing the key designation data** (i.e. random number) **to the authenticating means** (i.e. portable storage device) (0096, lines 3-6)**,**

a fifth step of performing the authentication with the authenticating means by using the first authentication key data (0099, lines 1-2).

As to claims 10, 13 and 14, Oishi discloses:

a second step of decrypting data-received from the means to be authenticated by using the decryption key data (0122, lines 1-3),

a third step of using data obtained by the decryption in the second step as the data that is effective, when verifying the means to be authenticated by the authentication in the first step (0107, lines 1-6).

Oishi fails to specifically disclose:

a first step of performing authentication with means to be authenticated by using second authentication key data, wherein the second authentication key data is generated from key data designated by key designation data, wherein the key designation data is from an integrated circuit ("IC") device, and wherein the IC device includes the first authentication key data generated using predetermined key data.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Oishi, as taught by Stirbu.

Stirbu discloses:

a first step of performing authentication with means to be authenticated by using second authentication key data (i.e. derived information), **wherein the second authentication key data is generated from**

key data designated by key designation data (i.e. secret key), **wherein the key designation data is from an integrated circuit ("IC") device, and wherein the IC device includes the first authentication key data generated using predetermined key data** (0033, lines 1-14).

Given the teaching of Stirbu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Oishi with the teachings of Stirbu by using data from an integrated circuit to authenticate processing devices. Please refer to the motivation recited above with respect to claim 1 as to why it is obvious to apply the teachings of Stirbu to the teachings of Oishi.

As to claim 11, Oishi discloses:

a fourth step of receiving at the data processing device the key designation data designating the predetermined key data from the means to be authenticated (0096, lines 7-11),

a fifth step of generating the second authentication key data by a second predetermined generation method by using the key data designated by the key designation data received in the fourth step (0096, lines 7-11)),

a sixth step of performing the authentication with the means to be authenticated using the first authentication key data for the authentication

by using the second authentication key data generated in the fifth step (0099, lines 1-2)**,**

a seventh step of verifying the means to be authenticated when judging that the first authentication key data and the second authentication key data by the authentication are the same in the sixth step (0107, lines 1-6)**.**

As to claim 12, Oishi discloses:

wherein, a function of the data processing device permitted by the means to be authenticated related to the predetermined key data, or an access to data held by the data processing device, is executed in the third step (0002, lines 1-7; 0142, lines 2-6). The examiner asserts that since Oishi discloses that audio and other data is protected from use without mutual apparatus identification, then one of ordinary skill in the art would understand that audio and other data would be available for use if mutual identification were successful.

As to claims 15-22, Oishi fails to specifically disclose:

wherein the first authentication key data is communicatively provided from the IC device to the first data processing device,

wherein the key designation data is communicatively provided from the IC device to the second data processing device.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Oishi, as taught by Stirbu.

Stirbu discloses:

wherein the first authentication key data is communicatively provided from the IC device to the first data processing device (0032, lines 5-8; 0033, lines 1-8)**,**

wherein the key designation data is communicatively provided from the IC device to the second data processing device (0033, lines 9-11)**.**

Given the teaching of Stirbu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Oishi with the teachings of Stirbu by using data from an integrated circuit to authenticate processing devices. Please refer to the motivation recited above with respect to claim 1 as to why it is obvious to apply the teachings of Stirbu to the teachings of Oishi.

As to claims 24 and 28, Oishi fails to specifically disclose:

wherein the mobile communication device is a cellular telephone.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Oishi, as taught by Stirbu.

Stirbu discloses:

wherein the mobile communication device is a cellular telephone (0085, lines 5-8)**.**

Given the teaching of Stirbu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Oishi with the teachings of Stirbu by using a cellular telephone as the mobile device. Stirbu recites motivation by disclosing that using a device that bears the ISIM card allows for complete implementation of functionality, but that it is well known that other kinds of UEs such as laptop computers connected to a MT or mobile router may be used (0085, lines 8-17). It is obvious that the teachings of Stirbu would have improved the teachings of Oishi by using a cellular telephone as the mobile communication device in order to implement complete functionality and communicate using a digital communication system.

Prior Art Made of Record

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ishiguro et al. (US Patent 7,237,112 B1) discloses a system and method for preventing recording data from being illicitly read out and analyzed.

b. Kanno et al. (US 2004/0049454 A1) discloses a system and method for electronic money settlement using a mobile communication terminal.

c. Takada et al. (US Patent 7,046,810 B2) discloses a system and method for data processing of portable device data.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431